

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-074408

(43)Date of publication of application : 18.03.1997

(51)Int.Cl.

H04L 9/08  
G09C 1/00  
G09C 1/00  
H04L 9/32

(21)Application number : 07-226267

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>  
N T T ELECTRON TECHNOL KK

(22)Date of filing : 04.09.1995

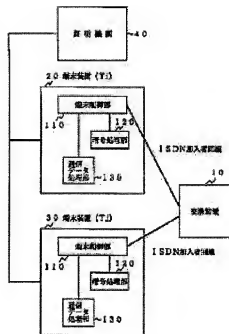
(72)Inventor : TANAKA KIYOTO  
AOKI KATSUHIKO

## (54) SECURITY COMMUNICATION METHOD

## (57)Abstract:

PROBLEM TO BE SOLVED: To eliminate an overhead for a verification procedure between terminal equipments and to prevent contradiction from being incurred between communication channels for ciphering/decoding communication data.

SOLUTION: Terminal equipments 20, 30 hold a certificate signed digitally by a private key of a verification agency 40 with respect to an identification name of the terminal equipments and digital information of a public key as information to verify it that the terminal equipments are correct. In the case of security communication by the terminal equipments 20, 30, at first a channel to verify the terminal equipments with each other is open and each certificate is exchanged mutually to confirm the correctness of the opposite party. Then a communication channel for ciphering/decoding of the communication data is open for a higher layer of the communication channel opened for verification and a secret key of the correct key ciphering system is used in common by using the open public key ciphering system.



特開平9-74408

(43) 公開日 平成9年(1997)3月18日

(51) Int.Cl. <sup>4</sup>	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 C
		7259-5 J		6 3 0 E
	6 4 0	7259-5 J		6 4 0 A
		7259-5 J		6 4 0 E
審査請求 未請求 請求項の数 4 O L (全 8 頁) 最終頁に続く				

(21) 出願番号 特願平7-226267

(22) 出願日 平成7年(1995)9月4日

(71) 出願人 000004226

日本電信電話株式会社  
東京都新宿区西新宿三丁目19番2号

(71) 出願人 591230295

エヌティティエレクトロニクステクノロジー  
株式会社  
東京都武蔵野市吉祥寺本町1丁目14番5号

(72) 発明者 田中 清人

東京都千代田区内幸町1丁目1番6号 日  
本電信電話株式会社内

(74) 代理人 弁理士 鈴木 誠

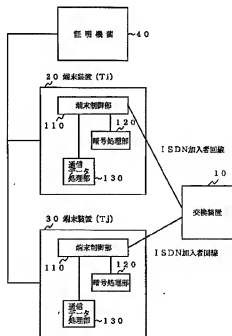
最終頁に続く

(54) 【発明の名称】 秘密通信方法

## (57) 【要約】

【課題】 端末相互の認証手順のオーバーヘッドをなくし、また、通信データの暗号化／復号のための通信路相互で矛盾を生じないようにする。

【解決手段】 端末装置 20、30 は、当該端末自身が生じたいことを証明するための情報として、端末の識別名と端末のパブリック鍵のデジタル情報に対して証明機関 40 のプライベート鍵によりデジタル署名された証明書を持保持する。端末装置 20、30 が秘密通信を行う場合、まず、相互に認証を行うための通信路を開設し、証明書を相互に交換して相手が生じたいと確認する。次に、上記認証のために開設した通信路の上位に通信データの暗号化／復号を行うための通信路を開設し、秘密鍵暗号方式の秘密鍵を公開鍵暗号方式を使用して共有する。



【特許請求の範囲】

【請求項1】 各端末装置は、端末装置自身が正しいことを証明するための情報として、端末装置の識別名と端末装置の公開鍵暗号方式におけるパブリック鍵とで構成されたデジタル情報に対して証明機関の公開鍵暗号方式のプライベート鍵によりデジタル署名された証明書保持し、端末装置相互が秘密通信を行うとき、まず端末装置が保持する前記証明書を相互に交換して相手が正しいと認証し、次に通信データの内容の暗号化/復号に使用するための秘密鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、該相互に共有した通信用の秘密鍵を使用して秘密通信を行う方法において、  
端末装置T1と端末装置Tjが秘密通信を行うとき、まず、端末装置T1、Tjは相互に認証を行うための通信路を開設し、自分を証明する証明書C1、Cjを互いに交換し検証することで、相手が正しいことを確認するとともに認証のために開設した通信路が正しいことを確認し、次に、認証のために開設した通信路上位に通信データの内容の暗号化/復号を行うための通信路を開設し、通信データの内容の暗号化/復号のための秘密鍵を共有するために、端末装置T1は乱数Rkviを発生し、該乱数Rkviを端末装置Tjの認証時に取得した証明書Cjから取り出した端末装置Tjのパブリック鍵を使用して暗号化するとともに、該暗号化データに対して端末装置T1のプライベート鍵で暗号化することでデジタル署名を行い、これら暗号化データとデジタル署名データのデジタル情報を端末装置Tjに送信し、  
前記デジタル情報を受信した端末装置Tjは受信したデジタル情報中の端末装置Tjのパブリック鍵により暗号化された乱数Rkviのデジタルデータを端末装置Tjのプライベート鍵により復号するとともに、該復号したデジタルデータと前記端末装置Tjのパブリック鍵により暗号化された乱数Rkviのデジタルデータを比較し、等しければ正しく端末装置T1より送信された秘密鍵情報であると確認し、  
次に、端末装置Tjは乱数Rkvjを生成し、該生成した乱数Rkvjと前記復号した乱数Rkviとの排他的論和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータとし、さらに前記乱数Rkvjを前記端末装置T1の認証時に取得した証明書C1から取り出した端末装置T1のパブリック鍵を使用して暗号化するとともに、該暗号化データに対して端末装置Tjのプライベート鍵で暗号化することでデジタル署名を行い、これら暗号化データとデジタル署名データデジタル情報を端末装置T1に送信し、  
前記デジタル情報を受信した端末装置T1は、受信したデジタル情報中の端末装置T1のパブリック鍵によ

り暗号化された乱数Rkvjのデジタルデータを端末装置T1のプライベート鍵により復号することにより乱数Rkvjの値を得るとともに、デジタル署名データを端末装置Tjの認証時に取得した証明書Cjから取り出した端末装置Tjのパブリック鍵を使用して復号し、該復号したデジタルデータと前記端末装置Tjのパブリック鍵により暗号化された乱数Rkvjのデジタルデータを比較し、等しければ正しく端末装置T1より送信された鍵情報であると確認し、

次に、端末装置T1は前記生成した乱数Rkviと前記復号した乱数Rkvjとの排他的論和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータとし、端末装置T1と端末装置Tjは、前記共有した秘密鍵と他のデータを使用して秘密鍵暗号方式で通信内容の暗号化ならびに復号を行うことを特徴とする秘密通信方法。

【請求項2】 請求項1記載の秘密通信方法において、通信データの内容の暗号化/復号のための通信路は、認証のために開設した通信路上位に複数開設可能し、各通信データの内容の暗号化/復号の通信路で秘密通信を行うときは、各々の通信データの内容の暗号化/復号のための通信路で秘密鍵を共有することで、一つの認証のための通信路上で、各々異なる秘密鍵を使用して複数の通信路で秘密通信を行うことを特徴とする秘密通信方法。

【請求項3】 請求項2記載の秘密通信方法において、通信データの内容の暗号化/復号のための通信路が、認証のための通信路上位に少なくともひとつ開設であれば、該認証のための通信路上に新しい通信データの内容の暗号化/復号のための通信路を開設するとき、秘密通信を行うために新たに必要な秘密鍵と他のデータを共有するために使用する証明書の情報は、既に開設している認証のための通信路の証明書の情報を使用することを特徴とする秘密通信方法。

【請求項4】 請求項3記載の秘密通信方法において、秘密通信を終了するとき、認証のための通信路上に開設された全ての通信データの内容の暗号化/復号のための通信路が開設されたときに、該認証のための通信路上の情報を閉鎖することを特徴とする秘密通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル伝送路を使用して端末装置間で秘密通信を行う方法に関し、特に、デジタル伝送路を使用して、データ情報を転送する場合にあたって好適な相互の認証方法ならびに通信内容の暗号化/復号に使用する鍵ならびにその他の秘密情報を共有する方法に関するものである。

【0002】

【従来の技術】デジタル通信のセキュリティ対策として秘密通信がある。秘密通信では、送信者と受信者が互いに相手が正しいと確認した上で秘密通信を行う。

3

【0003】秘話通信を行うための暗号方式は、大きく分けて、秘密鍵暗号方式と公開鍵暗号方式の二つがある。公開鍵暗号方式は、暗号化鍵と復号鍵が同じで、この同じ秘密鍵（以後秘密鍵と呼ぶ）を送信者と受信者が共有して相互に暗号化と復号を行う（詳細は、文献

【1】：「現代暗号理論：池野信一、小山謙二著、電子情報通信学会、P24~40、1988」を参照）。一方、公開鍵暗号方式は、暗号化鍵と復号鍵が異なり、復号鍵だけを秘密（以下プライベート鍵と呼ぶ）にするが、暗号化鍵を公開（以下パブリック鍵と呼ぶ）にする方式である（詳細は文献【1】：「現代暗号理論：池野信一、小山謙二著、電子情報通信学会、P77~104、1988」を参照）。

【0004】公開鍵暗号方式は、パブリック鍵を知っている誰もが秘話通信の送信者になれる点や、プライベート鍵を知っているただ一人が署名できる点で秘密鍵暗号方式より優れているが、計算量が膨大なため較符号化速度が遅いという欠点がある。このため現状では、送受信者相互の認証と通信データの内容の暗号化/復号の双方に秘密鍵暗号方式を使用するか（例えば、文献【2】：「山口他、LAN暗号通信の実装と評価、電子情報通信学会技術研究報告、OSF93-38、1993」を参照）、あるいは送受信者相互の認証には公開鍵暗号方式を使用し、通信データの内容の暗号化/復号には秘密鍵暗号方式を使用する（例えば、文献【3】：「J. Lin n. RFC1421: Privacy Enhancement for Internet ElectronicMail: Part1: Message Encryphon and Authentication Procedures. February 1993.」を参照）方法が使用されている。ここで、秘密鍵暗号方式ならびに公開鍵暗号方式による端末相互の認証方法については、例えば、文献【4】（「Information technology-Security techniques-Entity authentication-Part 2: Mechanisms using symmetric encipherment algorithms」ISO/IEC 9798-2:1994）や文献【5】：（「Information technology-Security techniques-Entity authentication-Part 2: Entity authentication using a public key algorithms」ISO/IEC 9798-3:1994）に詳述されている。これらの端末相互の認証を使用する従来方法では、認証後に秘話通信を行う場合、認証に使用した通信路そのものを通信データの内容の暗号化/復号に使用する。

【0005】

【発明が解決しようとする課題】上述の従来技術においては、既に秘話通信を行っている端末相互で、近大な論理パスを生成して秘話通信を行うには再度端末相互の認証を行わなければならない、オーバーヘッドが大きいという欠点がある。また、端末相互の認証に証明書を使用する場合、既に端末相互に認証ならびに秘密鍵の共有を終了し通信用のパスを確立して秘話通信を行っている時に、

4

新たにもう一つの通信用のパスを確立して秘話通信を行うには、次のような問題が生じる。すなわち、既設の秘話通信のための通信パスの確立のために互いに証明書の交換を行い認証を行ったときは相手の証明書の期限はまだ切れていなかったが、新たに開設する秘話通信のための通信用のパスのために相互に認証を行った時は、相手の証明書の期限が切れており、同じ端末同士で秘話通信を行うにもかかわらず、既設の通信用のパスは期限内であるが、新たに開設する通信用のパスは期限が切れているという状態不一致の問題が生じる。

【0006】本発明は、このような課題を解決しようとするものであり、その目的は、デジタル伝送路を使用し、データ情報を転送する場合にあたって好適な秘話通信の認証と鍵共有の方法を提供するものである。

【0007】

【課題を解決するための手段】本発明では、各端末装置は、端末装置自身が正しいことを証明するための情報として、端末の識別名と端末の公開鍵暗号方式に用いるパブリック鍵とで構成されたデジタル情報に対して証明機関の公開鍵暗号方式のプライベート鍵によりデジタル署名された証明書保持する。この証明書を保持する端末装置相互が秘話通信を行うとき、各端末装置は、以下のようにして、まず、端末装置が保持する証明書を相互に交換して相手方と正しいと認証し、次に、通信データの内容の暗号化/復号に使用するための秘密鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、この相互に共有した通信用の秘密鍵を使用して秘話通信を行う。

【0008】端末装置Tiと端末装置Tjが秘話通信を行うとする。まず、端末装置Ti、Tjは相互に認証するための通信路を開設し、自分を証明する証明書Ci、Cjを互いに交換し検証することで、相手方が正しいことを確認するとともに認証のために開設した通信路が正しいことを確認する。

【0009】次に、認証のために開設した通信路の上位に通信データの内容の暗号化/復号を行うための通信路を開設し、通信データの内容の暗号化/復号のための秘密鍵を共有するために、端末装置Tiは乱数Rkviを発生し、該乱数Rkviを端末装置Tjの認証時に取得した証明書Cjから取り出した端末装置Tjのパブリック鍵を使用して暗号化するとともに、該暗号化データまたは該暗号化データをハッシュしたデータに対して端末装置Tiのプライベート鍵で暗号化することでデジタル署名を行い、これら暗号化データとデジタル署名データのデジタル情報を端末装置Tjに送信する。

【0010】このデジタル情報を受信した端末装置Tjは、受信したデジタル情報中の端末装置Tjのパブリック鍵により暗号化された乱数Rkviのデジタルデータを端末装置Tjのプライベート鍵により復号することにより乱数Rkviの値を得るとともに、デジタル署名

5

データを端末装置T iの認証時に取得した証明書C iから取り出した端末装置T iのパブリック鍵を使用して復号し、該復号したデジタルデータと前記端末装置T jのパブリック鍵により暗号化された乱数R kviのデジタルデータを比較し、等しければ正しく端末装置T iより送信された秘密鍵情報であると確認する。次に、端末装置T jは乱数R kvjを生成し、この乱数R kvjと復号した乱数R kviとで排他的論理和をとり、該排他的論理和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータ（初期値）とする。さらに、端末装置T jは、該乱数R kvjを端末T iの認証時に取得した証明書から取り出した端末T iのパブリック鍵を使用して暗号化するとともに、該暗号化データまたは該暗号化データをハッシュしたデータに対して端末装置T jのプライベート鍵で暗号化することでデジタル署名を行い、これら暗号化データとデジタル署名データのデジタル情報を端末装置T iに送信する。

【0011】このデジタル情報を受信した端末装置T iは受信したデジタル情報中の端末装置T iのパブリック鍵により暗号化された乱数R kvjのデジタルデータを端末装置T iのプライベート鍵により復号することにより乱数R kvjの値を得るとともに、デジタル署名データを端末装置T jの認証時に取得した証明書C jから取り出した端末装置T jのパブリック鍵を使用して復号し、該復号したデジタルデータと前記端末装置T jのパブリック鍵により暗号化された乱数R kvjのデジタルデータを比較し、等しければ正しく端末装置T jより送信された秘密鍵情報であると確認する。次に、端末装置T iは、先に生成した乱数R kviと、乱数R kvjとで排他的論理和をとり、該排他的論理和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータ（初期値）とする。

【0012】これにより、端末装置T iと端末装置T jは、互いに等しい通信データの内容の暗号化に使用する秘密鍵とその他のデータ（初期値）を共有し、これらの共有した秘密鍵と他のデータを使用して秘密鍵暗号方式で通信内容の暗号化ならびに復号化を行う。

【0013】また、本発明では、通信データの内容の暗号化／復号の通信路は、認証のために開設した通信路の上位に複数本開設可能し、各通信データの内容の暗号化／復号の通信路で秘密鍵暗号方式で通信するとき、各々の通信データの暗号化／復号のための通信路で秘密鍵を共有することで、一つの認証のための通信路上で、各々異なる秘密鍵を使用して複数の通信路で秘密鍵暗号が可能とする。

【0014】さらに、本発明では、通信データの内容の暗号化／復号のための通信路が、認証のための通信路の上位に少なくともひとつ開設してあれば、該認証のための通信路上に新しい通信データの内容の暗号化／復号のための通信路を開設するとき、秘密鍵暗号方式で行うために新た

6

に必要な秘密鍵と他のデータを共有するために使用する証明書の情報は、既に開設している認証路の証明書の情報を使用する。

【0015】さらに、本発明では、秘密鍵通信を終了するときは、認証のための通信路上に開設された全ての通信データの暗号化／復号のための通信路が開設されたときに、該認証のための通信路上の情報を開設する。

【0016】

【実施例】以下、図面を参照して本発明の一実施例を説明する。なお、本実施例の説明ではデジタル伝送路としてISDNを用いるが、勿論、ISDN以外のデジタル伝送路でも適用可能である。

【0017】図1は、本発明の秘密鍵通信方法が適用される通信システムの一実施例を示すブロック図である。図1において、交換装置10は複数のISDN基本インタフェース加入者回線收容されている。端末装置20、30は該ISDN基本インタフェース加入者回線に接続されている。各端末装置は、ISDN加入者回線のレイヤ1～レイヤ3制御およびレイヤ4から上の上位レイヤのネットワーク制御を行う端末制御部110、端末相互の認証処理や鍵共有処理を行う暗号処理部120、共有した秘密鍵を使用して秘密鍵通信を行う通信データ処理部130から構成されている。端末装置20、30は証明機関40とも接続され、端末の識別名と端末のパブリック鍵で構成されたデジタル情報に対し、当該証明機関40のプライベート鍵によりデジタル署名された証明書（以下、証明書）の発行を受ける。なお、利用者が直接、証明機関40におもむいて証明書の発行を受ける場合には、端末装置20、30と証明機関40間の接続を省略できる。以下では、端末装置20をT i、端末装置30をT jとする。

【0018】図2に、本実施例の説明で使用する記号の一例を示す。なお、端末T jに関しては、図2の記号中の「i」を「j」に置き替えればよい。

【0019】図3は、証明機関40が作成する証明書の一例である。これは端末T iの証明書C iの例を示したもので、証明書の長さCDLと、端末装置の識別名Piと、端末T iの公開鍵暗号方式におけるパブリック鍵Pk iと、該T iとPk iを結合した情報に対して方向性のデータ圧縮関数Hでハッシュし、その値を当該証明機関40の公開鍵暗号方式のプライベート鍵Sc aで暗号化した暗号文E[Sc a](H(T i|| Pk i))、すなわち、デジタル署名されたデータで構成される。ここで、公開鍵暗号方式としては、代表的なものにRSA暗号方式（詳細は、文献[6]：「PKCS#1 RSA Encryption Standard, Version1.5, RSA Data Security Inc. 1993」を参照）があり、秘密鍵暗号方式としては、DES方式（詳細は、文献[7]：「FIPS Publication 46-1: Data Encryption Standard, National Bureau of Standards. 1988」を参照）がある。また、ハッシュ関数としては、MD2（詳細

は、文献[8]:「RFC1319: The MD2 Message-Digest Algorithm.», B. Kaliski., 1992」を参照)やMDS5(詳細は、文献[9]:「RFC1321: The MD5 Message-Digest Algorithm.», B. Kaliski., 1992」を参照)などがある。なお、本発明は、他の公開鍵暗号方式、秘密鍵暗号方式、ハッシュ関数に適用可能なことはもちろんである。

【0020】端末設置時に、端末装置20(端末T1)は、当該端末のパブリック鍵Pkiとプライベート鍵Skiを生成するとともに、該端末の識別名Tiとパブリック鍵Pkiを証明機関40に送って証明書Ciの発行の受け、該端末のプライベート鍵Ski、図2に示す証明書C1、証明機関40のパブリック鍵Pcaを暗号処理部120に設定する。同様に、端末装置30(端末T2)でも、該端末のプライベート鍵Skj、証明書Cj、証明機関40のパブリック鍵Pcaを暗号処理部120に設定する。

【0021】端末装置20(T1)と端末装置30(T2)が秘話通信を行うとき、まず、各端末が保持する証明書C1、Cjを相互に交換して相手が正しいことを認証し、次に、通信データの内容の暗号化/復号に使用するための秘話鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、この相互に共有した秘話鍵を使用して秘話通信を行う。

【0022】初めに、図4を用いて端末相互の認証手順を説明する。この段階ではすでに、端末T1は当該端末のプライベート鍵Ski、証明書C1、証明機関のパブリック鍵Pcaを保持し、端末T2でも当該端末のSkj、Cjおよび証明機関のPcaを保持している。

【0023】① 端末T1は乱数Riを生成し、端末T2にC1||Riを送信する。

② 端末T2は、受信した証明書C1を以下の通りに検査し、正しいことを確かめる。

- a. 受信したC1中のTi、PkiからH(Ti||Pki)を計算する。
- b. 受信したC1中のデジタル署名データからE[Pca](E[Sca]H(Ti||Pki)))を計算し、H(Ti||Pki)を得る。
- c. 上記aとbの計算値が等しいか検査し、等しいなら、受信した証明書C1は正しいと確認する。そして、正しいと確認されたら、受信した証明書C1を保持する。

【0024】④ 端末T2は乱数Rjを生成し、端末T1にCj||Rjを送信する。

④ 端末T1は、受信した証明書Cjを以下の通りに検査して、正しいことを確かめる。

- a. 受信したCj中のTj、PkjからH(Tj||Pkj)を計算する。
- b. 受信したCj中のデジタル署名データからE[Pca](E[Sca]H(Tj||Pkj)))を計算し、H(Tj||Pkj)を

得る。

- c. 上記aとbの計算値が等しいか検査し、等しいなら、受信した証明書Cjは正しいと確認する。そして、正しいと確認されたら、受信した証明書Cjを保持する。

【0025】⑤ 端末T2は端末T1に、Rj、Ri、T1の平文データとその暗号化データを結合したRj||Ri||Ti||E[Ski](Rj||Ri||Ti))を送信する。

⑥ 端末T1は、受信した情報を以下の通りに検査し、端末T2が正しいことを確かめる。

- a. 受信した暗号化データからE[Pki](E[Ski](Rj||Ri||Ti))を計算し、Rj||Ri||Tiを得る。
- b. 受信した平文データのRj||Ri||Tiと、上記aで得たRj||Ri||Tiとを比較する。等しければ、端末T2が正しいと確認する。

【0026】⑦ 端末T1は端末T2に、Ri、Rj、Tjの平文データとその暗号化データを結合したRi||Rj||Tj||E[Ski](Ri||Rj||Tj))を送信する。

⑧ 端末T2は、受信した情報を以下の通りに検査し、端末T1が正しいことを確かめる。

- a. 受信した暗号化データからE[Pki](E[Ski](Ri||Rj||Tj))を計算し、Ri||Rj||Tjを得る。
- b. 受信した平文データ中のRi||Rj||Tjと、上記aで得たRi||Rj||Tjとを比較する。等しければ、端末T1が正しいと確認する。

【0027】次に、図5を用いて、通信データの内容の暗号化/復号のために使用する秘密鍵とその他の必要データ(初期値)の共有手順について説明する。この段階では、端末T1は当該端末の証明書C1に加えて相手端末T2の証明書Cjを保持し、同様に端末T2でも当該端末のCjに加えて相手端末T1のC1を保持している。

【0028】① 端末T1は乱数Rkviを生成し、端末T2にRkviの暗号化データとそのデジタル署名データを結合したE[Pki](Rkvi)||E[Ski](H(E[Pki](Rkvi))))を送信する。

② 端末T2は、受信した情報を以下の通りに検査して、情報が正しいことを確かめ、データ暗号化鍵と初期値を生成する。

- a. 受信したデジタル署名データからE[Pki](E[Ski](H(E[Pki](Rkvi))))を計算し、H(E[Pki](Rkvi)))を得る。
- b. 受信した暗号化データからH(E[Pki](Rkvi)))を計算し、上記aで得たH(E[Pki](Rkvi)))と比較し、等しければ、メッセージが改ざんされていないと確認する。

c. E[Ski](E[Pki](Rkvi))を計算し、Rkviを得る。

- d. 乱数Rkviを生成する。そして、上記cで復号した乱数Rkviと生成した乱数Rkvjとで排他的論理和を取り、以下の通りにデータ暗号化/復号鍵DEKs、初期

9

値IVsを生成する。

DEKs: RkviとRkvjの排他的論理和データの上位8  
バイト

IVs: RkviとRkvjの排他的論理和データの低位8  
バイト

e. DEKsとIVsを通信データ処理部130へ設定す

【0029】③ 端末Tiは端末Tiに、Rkvjの暗号化  
データとそのデジタル署名データを結合したE[Pki]  
(Rkvj) || E[Skj] (H(E[Pki](Rkvj)))を送信す  
る。

④ 端末Tiは、受信した情報を以下の通りに検査し  
て、情報が正しいことを確かめ、データ暗号化鍵と初期  
値を生成する。

a. 受信したデジタル署名データからE[Pkj] (E[S  
kj] (H(E[Pki] (Rkvj))))を計算し、H(E[Pki] (R  
kvj))を得る。

b. 受信した暗号化データからH(E[Pki] (Rkvj))を  
計算し、上記aで復号したH(E[Pki] (Rkvj))と比較  
し、等しければ、メッセージが改ざんされていないと確  
認する。

c. E[Skj] (E[Pki] (Rkvj))を計算し、Rkvjを得  
る。

d. 上記cで復号した乱数Rkvjと先に生成した乱数Rk  
viとで排他的論理和を取り、以下の通りにデータ暗号化  
/復号鍵DEKs、初期値IVsを生成する。

DEKs: RkviとRkvjの排他的論理和データの上位8  
バイト

IVs: RkviとRkvjの排他的論理和データの低位8  
バイト

e. DEKsとIVsを通信データ処理部130へ設定す  
る。

【0030】以後、端末Tiと端末Tjは、共有した暗号  
化/復号のための秘密鍵DEKsとその初期値IVsを使  
用して通信データの暗号化/復号を行う。例えば、端末  
Tiが送信側、端末Tjが受信側の場合、端末Tiは平文  
(通信データ)pを鍵DEKs、初期値IVsで秘密鍵暗  
号方式により暗号化した暗号文e[DEKs, IVs](p)  
を生成して送信し、端末Tjは、受信した暗号文につ  
いて同じくDEKs, IVsで秘密鍵暗号方式によりd[DE  
Ks, IVs](e[DEKs, IVs](p))を計算して、  
平文pを復号する。

【0031】次に、図4の認証のための通信路ならびに  
図5の通信路が既に確立し、端末Tiと端末Tjの間で通  
信データの暗号化/復号を行っているときに、同  
じ端末間で新たな秘密通信要求が発生した場合の動作に  
ついて、図6により説明する。端末TiならびにTjは、  
互いに認証した相手端末の証明書CあるいはCI(以下  
では、Cを総称する)に加えて、認証のための通信路が  
どの端末と確立されているかを示すカウンタフラグFlg

10

jあるいはFigi(以下では、Flgで総称する)を保持し  
ている。初期状態ではカウンタフラグFlg、証明書Cと  
もゼロである。図6では、FlgとCが各々1個しか示さ  
れていないが、もちろん複数の端末と同時に秘密通信を  
行うために、複数のカウンタフラグFlgと証明書Cを保  
有することが可能である。

【0032】秘密通信の要求が発生したとき、端末はカ  
ウンタフラグFlgがゼロ以上かどうかと、ゼロ以上なら  
どの端末であるかを示す情報を含む証明書Cを検査する  
ことにより、端末の動作を決定する。すなわち、新たに  
秘密通信の要求が発生したとき、Flgを検査し、ゼロ  
以上かどうか調べる。Flgがひとつもゼロ以上でないな  
ら、または、Flgがゼロ以上でも、保有している証明書  
Cを検査した結果、秘密通信を行う相手の証明書Cを保  
持していないなら、新しい端末との秘密通信要求とし、  
前記の図4と図5の手順を実行して端末相互の認証と通  
信データの暗号化/復号を行うための鍵を共有  
し、秘密通信を行う。図6(a)はこれを示したもの  
で、便宜上、ここでは端末相互の認証手順のみを示して  
いる。このとき、Flgの内容は1加算するとともに、獲  
得した対応する端末の証明書Cを保持機構に設定する。

【0033】一方、新たに秘密通信の要求が発生したと  
き、検査したFlgがゼロ以上でかつ、秘密通信を行う相  
手の証明書Cを既に保持しているなら、対応するFlgの  
内容を1加算するとともに、図3で確立した認証のため  
の通信路上で、直ちに図5の鍵共有手順を実行し、新た  
な通信データの暗号化/復号のための通信路を確立する  
とともに、この通信路上で秘密通信を行うための鍵を共  
有する。このとき、相手端末の証明書Cは、既に保持し  
ている証明書を使用し、端末相互の新たな証明書はの交  
換は実行しない。図6(b)はこれを示している。

【0034】このようにすることにより、端末相互で1  
本の物理チャネル上に複数の論理パスを開設して秘密通  
信を行う場合においても、端末相互の認証は最初の1回  
で終了するとともに、論理パスごとに異なる鍵で通信デ  
ータの暗号化/復号を実行することができる。

【0035】次に、秘密通信を終了する場合について説  
明する。秘密通信を終了するときは、その要求にもとづ  
き、まず最初に該通信データの暗号化/復号のため  
の通信路を開設する。次に、図6に示したカウンタフ  
ラグFlgにおいて、開設した相手端末に対応するFlgの  
内容を1減算する。減算した結果がゼロ以上なら、図4  
で確立した認証のための通信路はそのままとし、その秘  
密通信終了のための要求動作を終了する。もしFlgの内  
容を1減算した結果がゼロなら、獲得している対応する  
端末の証明書Cの内容を初期化(クリア)するととも  
に、相手端末に対応する開設している図4の認証のため  
の通信路を開設することで、その秘密通信終了のための  
要求動作を終了する。

【0036】このようにすることにより、図4の認証の

11

ための通信路の上に複数の通信データの内容の暗号化／復号のための通信路が開設されているときは、認証のための通信路をそのままできるので、上記の、図4の認証のための通信路ならびに図5の通信路が既に確立し、通信データの内容の暗号化／復号を行っているときに、同じ端末間で新たな秘話通信要求が発生した場合の動作が実行できる。

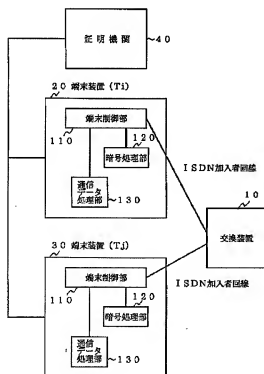
【0037】

【発明の効果】以上のように、本発明の認証および鍵共有方法によれば、既に秘話通信を行っている端末相互で、新たな論理パスを生成して秘話通信を行う特には、再度端末相互の認証を行う必要がないためオーバーヘッドがなく、また、証明書の通信データの内容の暗号化／復号のための通信パス相互で矛盾を生じないという利点がある。

【図面の簡単な説明】

【図1】本発明の秘話通信方法が適用される通信システ

【図1】



12

ムの一実施例を示すブロック図である。

【図2】本発明の実施例に使用する記号とその意味の一例を示す図である。

【図3】本発明で使用する証明書の一例を示す図である。

【図4】本発明による端末相互の認証手順を説明するための図である。

【図5】本発明による秘密鍵共有手順を説明するための図である。

【図6】本発明による新たな秘話通信要求が発生した場合の認証／秘密鍵共有手順を説明するための図である。

【符号の説明】

- 10 交換装置
- 20, 30 端末装置
- 40 証明機関
- 110 端末制御部
- 120 暗号化処理部
- 130 通信データ処理部

【図2】

記 号	意 義
Ti	端末Tiの識別名
Ri, Rkvi	端末Tiが発生する乱数
Ski	端末Tiのプライベート鍵
Pki	端末Tiのパブリック鍵
Scs	証明機関のプライベート鍵
Pcs	証明機関のパブリック鍵
DEKs	通信データの内容の暗号化／復号に使用する秘密鍵
I Vs	通信データの内容の暗号化／復号のための初期値
e[DEKs, I Vs](p)	平文pを鍵DEKs、初期値I Vsで秘密鍵暗号方式により暗号化した暗号文
d[DEKs, I Vs](c)	暗号文cを鍵DEKs、初期値I Vsで秘密鍵暗号方式により復号した平文
E[Ski](p)	文pを鍵Skiで公開鍵暗号方式により暗号処理した暗号文
E[Pki](E[Ski](p))	暗号文E[Ski](p)を鍵Pkiで公開鍵暗号方式により復号処理した復号文
H(p)	文pを関数Hでハッシュした値
	結合
CI	端末Tiの証明書

【図3】

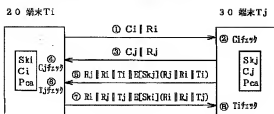
端末Tiの証明書CI

CDL
Ti
Pki
E[Scs](H(Ti    Pki))



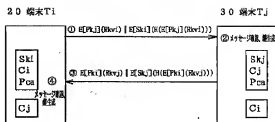
【図4】

## 端末相互の認証手順



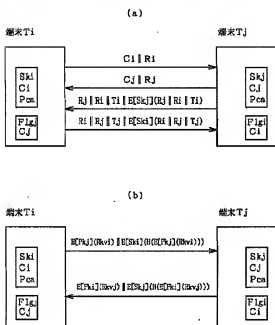
【図5】

## 鍵共有手順



【図6】

## 端末相互の認証／鍵共有手順



フロントページの続き

(51) Int. Cl.<sup>6</sup>

H 0 4 L 9/32

識別記号

庁内整理番号

FI

H 0 4 L 9/00

技術表示箇所

6 0 1 E

6 7 3 B

6 7 5 A

(72)発明者 青木 克彦

東京都武蔵野市吉祥寺本町1丁目14番5号

エヌティティエレクトロニクステクノ

ジー株式会社内